



Department of Homeland Security Daily Open Source Infrastructure Report for 25 April 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- NBC reports the Nuclear Regulatory Commission says the hole in a pipe at Florida Power and Light's Turkey Point Nuclear Power Plant was not an accident, but was likely caused by a disgruntled employee. (See item [5](#))
- Government Technology reports the University of Texas at Austin announced that an unknown person or persons has gained entry to the McCombs School of Business computers and gained unauthorized access to a large number of electronic records. (See item [14](#))
- The Chicago Sun–Times reports cameras and electronic fences that secure O'Hare International Airport have been malfunctioning in recent days, leaving portions of the airport potentially vulnerable. (See item [19](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *April 25, Belvoir Eagle (VA)* — **Engineer battalion assists in Virginia Beach.** Eight soldiers from the 249th Engineer Battalion (Prime Power) recently assessed the emergency power needs of more than 100 critically designated facilities in Virginia Beach, VA. “[249th Soldiers] are going around to these different facilities and doing an assessment of the electrical systems to

determine what size backup generator would be needed to bring the facility back up and operational in the event of a power grid failure,” explained Sgt. 1st Class Christopher Wooley, battalion operations sergeant. Critically designated facilities include hospitals, nursing homes, police and fire stations, town halls and schools that serve as shelters. The soldiers determined what size generator would be necessary to power each building by conducting electrical load calculations based on what each individual facility is used for. They also determined the best way to install a generator at each site. Capt. Frank Townsend said the exercise is a precursor to an event in May, which will simulate a hurricane striking Virginia Beach. Wooley estimated the assessments could reduce the amount of time it takes to get generators transported and installed at critically designated facilities, following a disaster, by six to eight hours.

Source: <http://www.belvoireagle.com/archives/2006/APR/20/249th.shtml>

2. *April 23, Associated Press* — **Edison switches on power plant near Los Angeles.** On Friday, April 21, Southern California Edison activated a natural gas–fueled generating plant in Redlands, CA, that will create 1,054 megawatts of electricity, or enough for 685,000 homes. Last year, there were some rotating blackouts because of power transmission problems coupled with high use of air conditioners. The plant, called Mountainview, is the first major electrical plant built in the Los Angeles area in 30 years, one of the fastest–growing areas in the country. Source: http://cbs2.com/local/local_story_113155735.html
3. *April 22, Bloomberg* — **China to receive first LNG shipment from Australia in May.** China, the world's biggest energy user after the U.S., will receive its first shipment of liquefied natural gas (LNG) from Australia next month as the country starts operating a receiving terminal for the fuel. China's demand for LNG is likely to increase as it boosts use of competitively priced and clean energy alternatives, said Don Voelte of Woodside Petroleum Ltd. China wants to more than double the share of its energy produced from gas to eight percent by 2010 to cut pollution and reduce the country's reliance on coal and crude oil. The \$600 million terminal, built by the nation's biggest offshore oil producer China National Offshore Oil Corp., will start commercial operations in June, Executive Vice Governor of Guangdong province Zhong Yangsheng, said. Demand from China and India for cleaner fuels will help global LNG consumption more than double to almost 400 million tons by 2015, said Daryl Houghton of the energy consulting company Poten & Partners Inc. Source: <http://www.bloomberg.com/news/markets/energy.html>
4. *April 21, MarketWatch* — **Grid operator approves three power line projects in northern California.** The California Independent System Operator (ISO) Thursday, April 20, approved three projects to improve the electric transmission system of northern California. The move had been expected. The projects still require the approval of the California Public Utilities Commission. The ISO hopes the improvements will lower costs and make the grid in northern California more reliable. The three major projects, developed by the ISO and Pacific Gas & Electric Corp., are a new transformer at the Vaca Dixon substation expected online December 2007, improvements to the 230–kilovolt lines from Vaca Dixon to the Tulacay and Lakeville substations, and a new 115–kV underground cable in Oakland. The last two projects are expected to be in service by May 2010. Source: <http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfi&siteid=google&guid=%7BA6705BCB-3D73-47E9-A18C-629D40D6C33F%7D&keyword=>

5. *April 21, NBC 6 (FL)* — **NRC Chair: Hole in pipe at Turkey Point not an accident.** On Friday, April 21, the chair of the Nuclear Regulatory Commission (NRC), Dr. Nils Diaz, said that cases of power plant sabotage are usually tracked to a disgruntled employee. In early April, a small hole was found in a coolant pipe at Florida Power and Light's Turkey Point Nuclear Power Plant. Though not saying that that was why a small hole was purposely drilled in a coolant pipe at Turkey Point Nuclear Power Plant, Diaz strongly hinted that that could be the case. "We do not believe it is an accident. We do believe the hole was drilled in there on purpose," Diaz said. He said it is not a major safety issue but it causes worries about security issues.

Source: <http://www.nbc6.net/news/8889092/detail.html>

6. *April 20, Canadian Press* — **Oilrigs seen as possible terrorist targets.** The Canadian military is working to prevent possible terrorist attacks against several giant oil and gas platforms currently drilling off the country's East Coast. Rear Admiral Dan McNeil said that various government agencies are trying to come up with defense strategies against possible scenarios that could leave the numerous rigs vulnerable to threats. Rear Adm. McNeil said the federal government has made preparing for such occurrences its top priority, despite the fact there are no perceived threats facing the nine rigs now sitting off Nova Scotia and Newfoundland. There are only about 100 people on the four of nine rigs that have manned crews. Rear Adm. McNeil said the military is preparing for attacks that could involve everything from small boats to aircraft or missiles. Several experts have suggested Canada isn't a top target for international terrorists and, if it were, Atlantic Canada's offshore rigs would likely not be at the top of their hit list. David Harris, a former strategic planner for the Canadian Security Intelligence Service, said the offshore operations are high-value targets that would have devastating economic impacts and be an effective psychological blow against North America.

Source: <http://www.theglobeandmail.com/servlet/story/LAC.20060420.RIGS20/TPStory/National>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

7. *April 24, Aviation Now* — **Input: RFP for Navy unmanned aerial system is expected in autumn.** Input, a federal information technology consulting agency, expects a draft or even formal request for proposals (RFP) for the U.S. Navy's Broad Area Maritime Surveillance unmanned aerial system in October or November, said Brian Haney, director of member services. Haney, at an Input conference Thursday, April 20, featuring the Navy's chief information officer, said the total program could be worth \$2 billion. Meanwhile, the Navy's worldwide force protection integrated logistics sustainment program should issue its RFP within a week or so, Haney said. The \$500 million initiative will provide full support for

procurement, integration, installation sustainment and training for Navy shore equipment.

Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/RFP04246.xml

8. *April 23, Aviation Now* — **Pentagon officials give green light to new KC-X tanker program.** The U.S. Air Force's replacement tanker program has languished for two years while enduring a blizzard of analyses, but KC-X is finally being launched with a contract award expected in mid-2007. The program will contain a few surprises. The contract award date already involves a slide of about three months — from spring 2007 to summer — beyond earlier projections. In addition, the initial request for information (RFI) will ask for input from service providers as well as prime contractors. The former are companies that would supply (on a pay-by-the-hour basis) tankers and crews for training, test and other missions conducted in the U.S. That would free Air Force aircraft and crews for overseas deployments and could reduce the number of tankers the military would need to buy. The RFI is expected to be released during this week's Aerial Refueling Systems Advisory Group conference in San Diego. Source: http://www.aviationnow.com/avnow/news/channel_awst_story.jsp?id=news/aw042406p2.xml
9. *April 21, Government Computer News* — **Air Force IT modernization ahead of schedule.** The Air Force's IT modernization effort is moving forward rapidly, and the service should reach its targets for 2012 ahead of schedule, the Air Force Chief Information Officer said Thursday, April 20. The Air Force's goal over the next six years is to go from a service-wide total of 1,700 separate systems and 19,000 applications to a better-integrated unit of 700 systems and 10,000 applications. The Air Force also is committed to investing in the recapitalization of its aging air fleet. But the agency is aiming for cost savings through smarter business operations and more sophisticated technology. Source: http://www.gcn.com/online/vol1_no1/40491-1.html
10. *April 19, European Leaders in Procurement* — **European ship groups form procurement pact.** A number of European shipyard groups have set up a procurement pact to make joint purchases. The companies — BAE Systems, DCN, Fincantieri, Navantia and VT Shipbuilding Limited — recently signed an agreement setting up the Warship European Procurement Club. Source: <http://online.europeanleaders.net/latest-news/2006/4/19/ship-groups-form-procurement-pact.html>
11. *April 17, Government Accountability Office* — **GAO-06-480R: Department of Defense Actions to Modify the Commercial Communications Satellite Services Procurement Process (Correspondence).** The Department of Defense (DoD) continues to rely on commercial satellite communications to plan and support operations. DoD use of commercial satellite bandwidth has increased over the past few years, making the department the largest single customer of commercial satellite bandwidth. In recent years, DoD's process for acquiring commercial satellite communications has received criticism for being lengthy, inflexible, and costly. DoD is now reexamining how it procures commercial satellite services to address these issues. The Government Accountability Office (GAO) was asked to summarize the actions that DoD has taken to date in revising its requirements and acquisition approach for commercial satellite services. To accomplish their objective, GAO analyzed DoD's December 2004 commercial satellite policy describing DoD's new approach for acquiring commercial satellite

communication services. GAO reviewed DoD's July 2005 report to Congress and analyzed the supporting cost-benefit analysis to determine the extent of the options DoD considered in its analysis for acquiring fixed satellite services. GAO did not validate the results of the cost-benefit analysis.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-480R>

[\[Return to top\]](#)

Banking and Finance Sector

12. *April 25, Channel Register (UK)* — **Virus writers get into cyber-extortion.** Incidence of cyber-blackmail attempts rose during the first three months of this year. Malicious hackers are moving away from 'stealth use' of infected computers -- stealing personal data, using infected computers as part of zombie networks -- to direct blackmailing of victims, according to a new report from Kaspersky Lab. The study, *Malware Evolution: January to March 2006*, cites cases where virus writers have either encrypted data or corrupted system information before demanding a ransom for safe return of data victims. The quantities demanded vary between \$50 and \$2,500. Kaspersky reports that hackers are adopting more sophisticated encryption schemes.

Malware Evolution Report: <http://www.viruslist.com/en/analysis?pubid=184012401>

Source: http://www.channelregister.co.uk/2006/04/21/kaspersky_malware_trends_update/

13. *April 24, Reuters* — **Washington Mutual to buy Commercial Capital.** Washington Mutual, Inc., the largest U.S. savings and loan, said it agreed to buy out Commercial Capital Bancorp, Inc. for \$983 million to strengthen its commercial and retail banking business. Analysts have expected banking consolidation in the affluent Southern California area. Many banks have reported strong growth in borrowing among small businesses, helping to offset slowing growth in borrowing among consumers. Last summer, Washington Mutual bought the credit-card lender Provident Financial Corp. for more than \$6 billion. In an interview with Reuters in November, Kerry Killinger, Washington Mutual's chairman and chief executive officer, said the bank would continue to seek acquisition targets.

Source: <http://www.nytimes.com/reuters/business/business-financial-washingtonmutual-commercial.html>

14. *April 23, Government Technology* — **Unauthorized access of computer records discovered at University of Texas at Austin.** The University of Texas at Austin officials announced that an unknown person or persons has gained entry to the McCombs School of Business computers and gained unauthorized access to a large number of McCombs' electronic records. University President William Powers Jr. said that the university had notified the attorney general and his Internet enforcement unit. The security violation was discovered late Friday, April 21. Some of an estimated 197,000 records were accessed. An investigation has determined that information from the business school's computer system was obtained as early as Tuesday, April 11, including some Social Security numbers and possibly other biographical data, including those of alumni, faculty, staff, and current and prospective students of the business school as well as corporate recruiters.

Source: <http://www.govtech.net/magazine/story.php?id=99286>

15. *April 23, Fort Worth Star–Telegram (TX)* — **Tax information may be easy to steal.** In a little-known security breach that is becoming more prevalent as more Americans use their computers to do their taxes, more returns can be downloaded like music or videos through computer file-sharing programs, which enable users to download files from others' computers with permission. All files in an open folder, like bank statements and checking account and medical records, are available if the files are not moved to closed and secure files. In an experiment conducted by Scott Green, a computer consultant, while using a file-sharing program and typing in the words "tax return," he found tax returns on computers where the users did not place their personal information into secure file folders on their hard drives. The tax returns were left in open folders, available to anyone who uses file-sharing software.
Source: <http://www.detnews.com/apps/pbcs.dll/article?AID=/20060423/BIZ01/604230301/1010/rss23>
16. *April 22, VNUNet* — **Financial data theft up 410 percent; huge surge in attacks over Easter weekend.** One in four security threats reported over Easter were aimed at stealing financial data, according to ScanSafe. The company said that the 48 hours prior to the Easter weekend was marked by unusual traffic patterns for malicious Internet traffic, and information theft attacks rose by 410 percent. "The latent level of malware targeting financial information has been gradually increasing over the past two months...However, the week leading up to the Easter holiday saw the highest rise we have ever seen," the company said. John Edwards of ScanSafe suggested that the attackers hoped that users would let their guards down leading up to the holiday weekend, and that the attacks used an unusual mix of old and new threats. Edwards added that surges of activity were traditionally based on a single threat, such as a worm or virus. However, 45 percent of attacks over Easter used old malware such as Trojan-Spy.Win32.Agent.eo, while the other 55 percent came from emerging threats such as Trojan-Spy.HTML.Bankfraud.ot.
Source: <http://www.computing.co.uk/vnunet/news/2154558/financial-the-ft-410-per-cent>
17. *April 22, Associated Press* — **ATMs in Massachusetts hit in skimming scam.** Police in Bellingham, MA, say users of an ATM there had their account numbers stolen in a skimming scam. Police said they know of ten people so far who've reported unauthorized withdrawals from their accounts. Thousands of dollars were taken. The scam was centered at a Bank of America machine. Police said they're unsure exactly how the thieves conducted the scam. Last year, a man was charged with withdrawing at least \$400,000 from ATMs in the Needham and Wellesley areas in a skimming scam.
Source: <http://www.wtnh.com/global/story.asp?s=4804370>
18. *April 21, Computing (UK)* — **Phishing attacks soar; lack of action by ISPs to blame.** Nearly half of phishing attacks are being directed at Internet banks outside of the U.S., according to new research. The survey by RSA Cyota shows that 49 percent of identity stealing scams are targeting banks in Europe and Asia. The number of attacks increased to 3,400 last month. Germany has seen the biggest increase in phishing, while the U.S. and UK still suffer the most from fraudulent e-mails and spoof Websites. Approximately 60 percent of all phishing attacks and spoof bank sites were hosted in the U.S., rather than well-known Internet crime hotspot such as Russia, China, or Brazil. RSA Cyota said lack of action by Internet service providers in taking down spoof Internet banking sites as the main reason criminals were hosting Websites in Western countries.

[\[Return to top\]](#)

Transportation and Border Security Sector

19. *April 24, Chicago Sun–Times* — Glitch hits O'Hare International Airport cameras.

Cameras and electronic fences that secure Chicago's O'Hare International Airport have been malfunctioning in recent days, leaving portions of the airport potentially vulnerable. A corrupted data file triggered the software problem impacting the 1,000–camera network that feeds video images to the O'Hare Communications Center in the basement of O'Hare's indoor parking garage. Whenever a door alarm goes off, video is supposed to be sent automatically to a dispatcher's console, pinpointing the location of the breach. The so-called "automatic trigger" feature was interrupted nearly two weeks ago, when the data file was corrupted, according to Andrew Velasquez, executive director of the city's Office of Emergency Management and Communications. "Instead of using the auto trigger, the operator simply has to dial up the video manually. That can be done instantaneously when the alarm goes off and the signal is sent. It's a simple point–and–click function," Velasquez said. "The video can still be viewed within seconds. In no way shape or form was security at O'Hare compromised as a result of this issue." The software problem was finally repaired late last week, Velasquez said.

Source: <http://www.suntimes.com/output/news/cst-nws-hare24.html>

20. *April 24, NBC10 (PA)* — Underground fire shuts down Philadelphia's SEPTA subways. An overnight fire in Philadelphia's Southeastern Pennsylvania Transportation Authority (SEPTA) electrical room at 15th and Market streets shut down its subway service for a while early Friday morning, April 21. Commuters who depended on the Broad Street subway line were forced to take buses.

Source: <http://www.nbc10.com/news/8879789/detail.html>

21. *April 24, Transportation Security Administration* — Twelve canine teams graduate TSA's explosives detection course. The Transportation Security Administration (TSA) announced on Monday, April 24, the graduation of 12 new members of its National Explosives Detection Canine Team Program (NEDCTP). The teams will be assigned to mass transit systems in Washington DC (Washington Metropolitan Area Transit Authority); San Francisco (Bay Area Rapid Transit); Los Angeles (Los Angeles County Metropolitan Transportation Authority); and San Diego (San Diego Trolley, Inc.); and airports in Norfolk, VA, El Paso, TX, Tucson, AZ, Waianae, HI, and Milwaukee, WI. "The graduation of these 12 teams represents a major milestone," said Dave Kontny, NEDCTP's Director. "We now have approximately 400 canine teams from coast–to–coast, in both mass transit and aviation. We look forward to continuing our partnership with local law enforcement in this important program." Once the teams return to their airports and mass transit systems, they will undergo several hours of proficiency training each week that includes all the sights, sounds and distractions associated with these busy environments. Within the next few months, the teams will also undergo a rigorous on–site certification process. To ensure they maintain a high level of proficiency, the handlers and their dogs are re–certified annually in a stringent, three–to–four–day process.

Source: http://www.tsa.gov/public/display?theme=44&content=090005198_01d0597

22. *April 22, Associated Press* — **Delta: Pilot deal will aid reorganization.** Delta Air Lines Inc. executives said Saturday, April 22, that the roughly \$280 million in average annual concessions approved by leaders of its pilot union is less than the airline wanted, but it agreed to the deal because of the likelihood the pilots' pension plan will be terminated. A company statement did not say how it arrived at that figure, which includes a 14 percent wage cut, but it said Delta believes the cuts are enough to help it successfully reorganize in bankruptcy. "It also represents additional hardship for our pilots and I appreciate their consideration of something that is vitally important to the future of this company," Chief Executive Gerald Grinstein said. Rejection by the pilots could revive the threat of a strike against the nation's No. 3 carrier. If they approve it, the deal would go to the bankruptcy court for approval. Delta, which filed for bankruptcy in September, has said its pilots who worked a full year in 2005 earned an average of \$157,000.

Source: http://biz.yahoo.com/ap/060422/delta_pilots.html?.v=8

23. *April 18, Associated Press* — **Continental hires Chautauqua Airlines.** Continental Airlines Inc. on Tuesday, April 18, said it has contracted with Chautauqua Airlines to operate 69 regional jets that were previously run by ExpressJet Airlines Inc. Chautauqua is a unit of Republic Airways Holdings Inc., which provides connecting flights for major carriers including American Airlines, Delta, and US Airways. Financial terms of the deal were not disclosed. In December, Continental — ExpressJet's primary customer — warned the regional carrier that it planned to withdraw 69 aircraft from its capacity purchase agreement. ExpressJet is now required to notify Continental by September 28 whether it will keep any of the 69 planes or cancel the subleases and return the planes to Continental.

Source: http://biz.yahoo.com/ap/060418/continental_expressjet.html?.v=1

[\[Return to top\]](#)

Postal and Shipping Sector

24. *April 24, Yahoo! Finance* — **UPS profit up in first quarter.** United Parcel Service Inc.'s (UPS) first-quarter net income rose 10 percent to \$975 million, or 89 cents per share, diluted, from \$882 million, or 78 cents per share, a year ago. The Atlanta-based package shipper said the growth was driven by a nine percent increase in global small-package volume. During a conference call with analysts, UPS chief financial officer Scott Davis said company officials were disappointed with a \$34 million decline in operating profit in its Supply Chain Solutions and freight-forwarding operations. UPS chief financial officer Scott Davis chalked the decline up to roughly \$20 million in costs related to the integration of Menlo Worldwide Forwarding Inc. operations into the UPS network. UPS bought Menlo in December 2004 for \$150 million in cash and the assumption of about \$110 million in debt. UPS is in the process of completing an \$82 million, 700,000-square-foot heavy-freight air hub at Louisville International Airport. Davis also said UPS will move into the next phase of its integration of Overnite Corp., a truckload and less-than-truckload carrier it acquired in August 2005.

Source: <http://biz.yahoo.com/bizj/060421/1275391.html?.v=3>

[\[Return to top\]](#)

Agriculture Sector

25. *April 24, Food and Agriculture Organization of the United Nations* — **New version of the Food and Agriculture Organization GeoNetwork launched.** The Food and Agriculture Organization (FAO) recently launched a new version of its spatial data catalogue, FAO GeoNetwork, which provides agricultural information to decision-makers, allowing them to access satellite imagery, interactive maps and spatial databases from FAO, World Food Program, the Consultative Group on International Agricultural Research, and others. Users overlay maps from multiple servers housed at development institutions worldwide to create customized thematic maps on their own computers covering such variables as land cover, soil quality, vegetation, and population density and marketing access. The launch coincides with the release of a new version of the World Food Program GeoNetwork, which contributes substantially to the effective sharing and dissemination of geographical datasets with major emphasis on food security and vulnerability issues. The joint launch marks the start of a new era for spatial data sharing among UN agencies, allowing users to instantly see maps and related information from the different agencies together in one search.
Source: http://www.agprofessional.com/show_story.php?id=39939
26. *April 20, Associated Press* — **More brucellosis on feedgrounds.** A survey by the Wyoming Game and Fish Department suggests that 14 percent of the elk wintering on the National Elk Refuge near Jackson have been exposed to brucellosis, a far higher rate than in areas where the state doesn't feed elk during the winter. The department drew samples from elk shot by hunters last fall. While 14 percent of the elk on the refuge and in Grand Teton National Park showed exposure to brucellosis, the agency said surveys in southwest Wyoming, where elk aren't fed, showed a rate of exposure lower than one percent. The survey also tested bison killed by hunters in Jackson Hole. It found 66 percent of the animals were positive for exposure to the disease, compared to a five-year average of 60 percent. In the recent survey, successful hunters on the elk refuge and the national park submitted 182 usable blood samples, of which 14 percent tested positive for exposure to the disease. Only one elk out of 343 tested in southwest Wyoming during the same hunting season showed exposure to the disease, the department says. A similar survey of elk in northeast Wyoming the year before found no exposed elk.
Source: <http://www.jacksonholestartrib.com/articles/2006/04/20/news/wyoming/4afb6487b8fa601b872571540080ee71.txt>
27. *April 19, Agriculture Online* — **New report examines North American animal agriculture.** The U.S. livestock production system is competitive in world markets, but it's facing significant opportunities and challenges in North America and abroad, according to a study released Tuesday, April 18, by the Farm Foundation. The 18-month study, involving more than 150 individuals from Canada, Mexico, and the U.S. is believed to be the first to take a comprehensive look at the opportunities and challenges facing the major species of the animal agriculture industry in these three countries. Study participants examined the industry's challenges and opportunities in seven basic areas: economics of production, processing and marketing; consumer demands; global competitiveness and trade; food safety and animal health; environmental issues; community and labor; and animal welfare. Cross-cutting themes, strategies and policy issues which emerged include:
Full report and executive summary:
<http://www.farmfoundation.org/projects/04-32ReportTranslations.htm>.

Source: http://www.agriculture.com/ag/story.jhtml;jsessionid=VOKHFGM YCGY2JQFIBQPSAOQ?storyid=/templatedata/ag/story/data/1145466_705539.xml

[\[Return to top\]](#)

Food Sector

28. *April 20, Food Safety and Inspection Service* — **Tennessee firm recalls under-processed chicken fillets.** Perdue Farms is voluntarily recalling approximately 20,610 pounds of fully cooked breaded chicken breast fillets due to possible under-processing, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, April 20. The chicken breast fillets were produced on January 20, 2006 and March 4, 2006 and shipped to foodservice distribution centers in Indiana, Massachusetts, Missouri, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Tennessee and Utah. The problem was discovered by customers. FSIS has received no reports of illnesses from consumption of these products. Source: http://www.fsis.usda.gov/News & Events/Recall_014-2006_Release/index.asp

29. *April 20, Food Safety and Inspection Service* — **China added to list of countries eligible to export processed poultry to the U.S.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) on Thursday, April 20, announced a final rule making the People's Republic of China eligible to export processed poultry products from approved sources to the U.S. The final rule will allow export from China of processed poultry products derived from poultry raised in the U.S. and slaughtered in FSIS-inspected establishments or raised and slaughtered in other countries eligible to export poultry to the U.S. This rule does not make China eligible to export processed poultry products to the U.S. that are derived from birds of Chinese origin slaughtered in China's domestic establishments. The rule becomes effective on May 24. Certified establishments in China must have procedures to ensure that products produced for domestic use are processed at separate times from those produced for export to the U.S. FSIS will verify that establishments certified by China are meeting U.S. requirements. All processed poultry products exported to the U.S. from China will be subject to FSIS reinspection procedures at ports of entry. Final Rule: <http://www.fsis.usda.gov/Regulations & Policies/index.asp> Source: http://www.fsis.usda.gov/News & Events/NR_042006_01/index.asp

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

30. *April 24, Reuters* — **Africans told to step up bird flu cooperation.** African scientists must step up cooperation to fight bird flu, with lack of information almost as dangerous as lack of resources as the continent faces its next big health threat, a regional meeting heard on Monday,

April 24. Mazlan Jusoh, the UN Food and Agriculture Organization country representative for Malawi, said that although most countries in Africa remained free of the virus officials should boost surveillance now. Jusoh said countries must step up public awareness campaigns and put in place rapid response mechanisms to reduce the social and economic impact of the disease. Source: <http://www.alertnet.org/thenews/newsdesk/L24775445.htm>

31. *April 23, Kuwait News Agency* — **Over 40,000 birds culled in Pakistan following bird flu outbreak at 13 farms.** Authorities in Pakistan have culled over 40,000 birds following an outbreak of deadly H5N1 avian influenza strains at about 13 poultry farms on the outskirts of the capital city. Official sources told the Kuwait News Agency Sunday, April 23, that blood samples tested at the National Reference Laboratory (NRL) have confirmed the presence of bird flu at about 13 poultry farms in Tarlai and Alipur Farash areas. Officials said five more farms with suspected H5N1 strains have been quarantined and samples sent to the NRL for the outbreak confirmation. Source: http://www.kuna.net.kw/Home/Story.aspx?Language=en&DSNO=8554_29

32. *April 23, National Institutes of Health* — **Scientists design potent anthrax toxin inhibitor.** Scientists funded by the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health (NIH), have engineered a powerful inhibitor of anthrax toxin that worked well in small-scale animal tests. "This novel approach to the design of anthrax antitoxin is an important advance, not only for the value it may have in anthrax treatment, but also because this technique could be used to design better therapies for cholera and other diseases," says NIH Director Elias A. Zerhouni, M.D. The research appears in the Sunday, April 23, online edition of the journal *Nature Biotechnology*. Led by NIAID grantees Ravi S. Kane, Ph.D., of Rensselaer Polytechnic Institute, in Troy, NY, and Jeremy Mogridge, Ph.D., of the University of Toronto, the investigators built a fatty bubble studded with small proteins that can cling tightly to the cell membrane receptor-binding protein used by anthrax toxin to gain entry into a host cell. The protein-spiked fatty bubble, or "functionalized liposome," hampers a critical early step in the assembly process that anthrax toxin must undergo to become fully active. In test-tube experiments, the inhibitor, which is covered with multiple short proteins (peptides), was 10,000 times more potent than unattached peptides. The study, "Statistical pattern matching facilitates the design of polyvalent inhibitors of anthrax and cholera toxins," can be found at: <http://www.nature.com/nbt/journal/vaop/ncurrent/pdf/nbt1204.pdf> Source: <http://www.nih.gov/news/pr/apr2006/niaid-23.htm>

33. *April 22, New Straits Times (Malaysia)* — **Fever may be airborne, say officials.** The number of National Service trainees who have come down with high fever at a camp in Alor Gajah, in Malacca, Malaysia, has risen to 94 and health authorities suspect the disease is airborne. It was reported Friday, April 21, that 81 trainees had come down with high fever since Monday, April 17, with 25 admitted to the Malacca Hospital since Wednesday, April 19. The number under quarantine has now reached 69. They have "acute upper respiratory infection" and besides fever, they also have sore throat and coughs. Blood samples have been sent to the Institute of Medical Research in Kuala Lumpur and Sungai Buloh Hospital for analysis. Source: http://www.nst.com.my/Current_News/nst/Saturday/National/20060422123212/Article/index.html

34. *April 22, Center for Infectious Disease Research & Policy (University of Minnesota)* — **Addition of Egyptian cases raises avian flu tally to 204.** The World Health Organization (WHO) Friday, April 21, recognized eight human cases of H5N1 avian influenza previously reported in Egypt, pushing the global case count to 204, with 113 deaths. The Egyptian government has been reporting a total of 12 human cases, but until Friday, the WHO had listed only four cases in Egypt. Egypt's health ministry classifies cases as confirmed when samples test positive in the country's national public health laboratory and the U.S. Naval Medical Research Unit 3 in Cairo, the WHO said. All the cases confirmed in those two labs have now been validated by the WHO's collaborating lab in Britain, the agency said. Of the 12 Egyptians who suffered H5N1 infections, four have died and one remains hospitalized in stable condition, the WHO said, adding, "Seven patients have fully recovered and been discharged from hospital."

WHO statement on Egypt: http://www.who.int/csr/don/2006_04_13/en/index.html

Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/april2106avian.html>

35. *April 20, RadioFreeEurope/RadioLiberty* — **Tajikistan: Reappearance of leptospirosis in more than a decade.** At least 15 people have been hospitalized in Tajikistan with a potentially deadly bacterial disease called leptospirosis. The disease is generally transmitted through contact with animals or tainted water. The flu-like symptoms can be nearly nonexistent or misleading, but the risk to humans is very real. Experts say about one in 10 patients is likely to suffer major organ damage, and 3–5 percent of cases are fatal. The Tajik cases represent the first outbreak in this part of Central Asia in more than a decade. Health officials at the scene suspect the sudden infections might be the result of recent work on the public water system.

Source: <http://www.rferl.org/featuresarticle/2006/04/de7f1048-7a35-4976-9b5d-a934ca30ecf7.html>

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

36. *April 23, Express-News (TX)* — **Texas' top search team gets set for hurricane season.**

Instead of having members of the state's elite search and rescue team respond to mock terrorist attacks or the usual earthquake disaster practice, as it had done for many years, the state drilled team members on a hurricane catastrophe that featured many of the same obstacles encountered during Hurricanes Katrina and Rita Saturday, April 22. It was the first time in the nine-year history of Texas Task Force 1 that a full-size hurricane exercise was being carried out at Disaster City, a 52-acre training facility southwest of the Texas A&M University campus. "Although we regularly train in San Antonio, this facility in particular is very hard to duplicate and is the best substitute for a real-world event," said Nim Kidd, a San Antonio firefighter and the Alamo City's emergency management coordinator.

Source: http://www.mysanantonio.com/news/metro/stories/MYSA042306.02B.disaster_city.2fc703d.html

37. *April 22, Associated Press* — **Gulf Coast leaders will have hurricane evacuation group.** The 150 mayors and county judges in the 13-county region balked at Texas Governor Rick Perry's recent order that one person be given the authority to order hurricane evacuations. Instead, they voted to form a 15-member committee they said will better represent everyone's needs. Gulf Coast leaders have assured Governor Perry that their regional committee for disaster response will have a point person for hurricane evacuations.

Source: <http://www.click2houston.com/news/8910577/detail.html>

38. *April 22, Birmingham News (AL)* — **Alabama governor wants school buses activated for hurricanes.** Governor Bob Riley wants to use public school buses to speed up the evacuation of coastal areas the next time a major hurricane threatens Alabama. Riley said that, under evacuation plans being developed, school buses would run their normal routes. But instead of picking up kids with book bags, they'd be loading anyone who wants transportation to a shelter. Alabama is looking at doing several things differently during the upcoming hurricane season, from using school buses for evacuation to using community colleges for shelters.

Source: <http://www.al.com/news/birminghamnews/index.ssf?/base/news/1145728522125570.xml&coll=2>

39. *April 22, Press-Register (AL)* — **FEMA chief praises Alabama's preparedness.** Alabama's emergency planners Friday, April 21, worked through a worst-case scenario exercise — a Category 5 storm that traveled up Mobile Bay — and earned praise from a top federal official. "I'm extremely pleased at how well the state is prepared," said David Paulison, acting director of the Federal Emergency Management Agency (FEMA). "I wish every state in the country was doing this." Officials said the simulation, dubbed "Hurricane Craig," was bigger and more complex than previous drills, and Governor Bob Riley unveiled other improvements to the state's preparations at an afternoon news conference in the Capitol. Riley and Paulison met for four hours behind closed doors Friday with more than 100 people. Among changes for the 2006 hurricane season, the governor said more supplies will be pre-positioned at shelter sites and other items will be stockpiled at Maxwell Air Force Base in Montgomery rather than in Tennessee or Kentucky. Riley also said government officials will be able to place generators at gas stations and grocery stores in a storm's immediate aftermath.

Source: <http://www.al.com/news/mobileregister/index.ssf?/base/news/1145727979125590.xml&coll=3>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

40. *April 24, Info World* — **Rootkit programs benefit from open source.** An active, open source development community and new tools are fueling stealth "rootkit" programs. The number of stealth techniques found in malicious software surged 600 percent in the past three years, according to data published last week by McAfee. And the pace of change is accelerating, driven by developer interest and online forums, say experts.

Source: http://www.infoworld.com/article/06/04/24/77521_17NNrootkitp_lugnplay_1.html

41. *April 24, Associated Press* — **Pioneering Wi-Fi city sees startup woes.** More than a month after St. Cloud launched what analysts say is the country's first free citywide Wi-Fi network, folks in this 28,000-person Orlando, FL, suburb are still paying to use their own Internet service providers as dead spots and weak signals keep some residents offline and force engineers to retool the free system. The same troubles with the small town's big Internet project could be lessons for municipalities from Philadelphia to San Francisco considering similar networks. St. Cloud officials are spending more than \$2 million on a network they see as a pioneering model for freeing local families, schools and businesses from monthly Internet bills. It also promises to help the city reduce cell-phone bills and let paramedics in an ambulance talk by voice and video to hospital doctors. Instead, what they have so far is a work in progress. Several cities have Wi-Fi hotspots, but St. Cloud's 15-square-mile network is the first to offer free access citywide, said Seattle-based technology writer Glenn Fleishman, who runs a Website called Wi-Fi Networking News.

Source: http://news.yahoo.com/s/ap/20060424/ap_on_hi_te/muni_wi-fi_hiccups:_ylt=AspmQWkyYyR3gKDp43IxM8jtBAF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

42. *April 24, Associated Press* — **Seven Asian mobile companies form alliance.** Seven Asian mobile phone operators have formed an alliance to work together to promote voice, video and data roaming among the networks, the companies said Monday, April 24. With a combined customer base of 100 million people, the alliance consists of NTT DoCoMo of Japan, Hutchison Telecom Hong Kong, Far Eastone Telecommunications Co. of Taiwan, Hutchison Essar of India, KT Freetel Co. of South Korea, PT Indosat of Indonesia and StarHub of Singapore.

Source: http://news.yahoo.com/s/ap/20060424/ap_on_bi_ge/asian_mobile_alliance:_ylt=AuUHrjLlxSjh4Gt63wfvIM8jtBAF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

43. *April 24, VNUNet* — **Security giants converge on London for annual conference.** Over 10,000 attendees will descend on 300 exhibition stalls at the annual Infosecurity conference in Olympia, London, which kicks off Tuesday, April 25. Hot on the agenda will be the final results of the DTI's biannual UK IT crime survey, one of the most extensive of its type. But the unofficial champion of the conference and exhibition will be Gary McKinnon, the man accused of hacking into the U.S. Navy's computers in search of evidence for UFOs.

Source: <http://www.vnunet.com/vnunet/news/2154611/security-businesses-converge>

44. *April 23, USA Today* — **Malicious-software spreaders get sneakier, more prevalent.** At the height of his powers, Jeanson James Ancheta felt unstoppable. From his home in Downey, CA, the then-19-year-old high school dropout controlled thousands of compromised PCs, or "bots," that helped him earn enough cash in 2004 and 2005. But Ancheta got caught. In the first case of its kind, he pleaded guilty in January to federal charges of hijacking hundreds of thousands of computers and selling access to others to spread spam and launch Web attacks. In separate cases, federal authorities last August also assisted in the arrest of Farid Essebar, 18, of Morocco, and last month indicted Christopher Maxwell, 19, of Vacaville, CA, on suspicion of similar activities. The arrests underscore an ominous shift in the struggle to keep the Internet

secure: Cybercrime undergirded by networks of bots — PCs infected with malicious software that allows them to be controlled by an attacker — is soaring. Bot networks have become so ubiquitous that they've also given rise to a new breed of low-level bot masters, typified by Ancheta, Essebar and Maxwell. Tim Cranton, director of Microsoft's Internet Safety Enforcement Team, calls bot networks "the tool of choice for those intent on using the Internet to carry out crimes."

Source: http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-04-23-bot-herders_x.htm?POE=TECISVA

- 45. April 21, Security Focus — Symantec Scan Engine multiple vulnerabilities.** Three vulnerabilities have been discovered in the Symantec Scan Engine. The Scan Engine is a TCP/IP server and programming interface that enables third parties to incorporate support for Symantec content scanning technologies into their proprietary applications. This gateway-level product should not be confused with Symantec's desktop product. Analysis: The Symantec Scan Engine fails to properly authenticate Web-based user logins. Anyone with knowledge of the underlying communication mechanism can control the Scan Engine server. Symantec Scan Engine uses a static private DSA key for SSL communications. This key cannot be changed by end users and is easily extracted. This opens the product to a potential man-in-the-middle attack. Products affected: Symantec Scan Engine 5.0.

Solution: Symantec Engineers have verified these issues and have added fixes to the latest product update (5.1). Symantec strongly recommends all customers immediately apply the latest updates for their supported product versions to protect against these types of threats. Symantec Scan Engine updates are available through the Platinum Support Website for Platinum customers or through the FileConnect-Electronic Software Distribution Website for all licensed users.

Platinum Support Website: <https://www-secure.symantec.com/platinum/login.html>

FileConnect: <https://fileconnect.symantec.com/licenselogin.jsp>

Symantec April 21, 2006 advisory:

<http://www.symantec.com/avcenter/security/Content/2006.04.21.html>

Source: <http://www.securityfocus.com/archive/1/431734>

- 46. April 21, Computer World — New York county enacts wireless security law.** Westchester County, NY, last week enacted a new law that requires local businesses to implement "minimum security measures" for protecting their wireless networks. The law, which is believed to be the first of its kind anywhere in the country, applies to all commercial businesses that collect customer information, such as Social Security numbers, credit card or bank account information, and that also have a wireless network. Also covered by the law are businesses that offer public Internet access. The mandate was introduced as a measure to protect consumers against identity theft and other types of computer fraud, according to a statement posted on the county's Website. Businesses that collect, store and use personal information have 180 days to comply with the law.

Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,110762,00.html?SKC=security-110762>

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of publicly available exploit code and materials explaining how to exploit a race condition vulnerability in Sendmail. Sendmail improperly handles asynchronous signals causing a race condition vulnerability. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user. For more information please review the following:

TA06-081A – Sendmail Race Condition Vulnerability

<http://www.us-cert.gov/cas/techalerts/TA06-081A.html>

VU#834865 – Sendmail contains a race condition

<http://www.kb.cert.org/vuls/id/834865>

Sendmail MTA Security Vulnerability Advisory

<http://www.sendmail.com/company/advisory/>

US-CERT recommends the following actions to mitigate the security risks:

Upgrade to the latest version: Sendmail 8.13.6.

<http://www.sendmail.org/releases/8.13.6.html>

Review the Sendmail MTA Security Vulnerability Advisory for steps to reduce the impact of this vulnerability. <http://www.sendmail.com/company/advisory/#mitigation>

US-CERT is not aware of any working exploit code at this time.

Phishing Scams

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 445 (microsoft-ds), 139 (netbios-ssn), 135 (epmap), 53 (domain), 1025 (win-rpc), 80 (www), 1027 (icq), 1434 (ms-sql-m), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

47. April 24, USA TODAY — Levees not fully ready for hurricane season. All day, every day and into the night, crews for the U.S. Army Corps of Engineers pour concrete into walls, pack dirt into hills and ram steel into the earth. They are scrambling to undo the damage Hurricane Katrina inflicted on the region's levee system. Their task is urgent: Hurricane season begins June 1. But even when the holes are plugged -- a \$2 billion endeavor -- the entire 350-mile protection system remains flawed, the corps now admits. Flood walls are too weak in some places; earthen levees are too short in others. Corps officials are confident that by June, they will repair the breaches and other damage incurred along almost half the levee system. Lt. Gen. Carl Strock, commander of the corps, announced April 12 that the agency wants to correct and strengthen the entire system to withstand storms stronger than Katrina, which was a Category 3 when it made landfall the morning of August 29 in Plaquemines Parish. For this year's storm season, which lasts six months and promises to be active, the corps will not be able to upgrade the 181 miles of levees that remained intact during Katrina.

Source: http://www.usatoday.com/news/nation/2006-04-23-levees_x.htm

[[Return to top](#)]

General Sector

48. April 24, Associated Press — Three blasts rock Egypt resort, at least 18 killed. Three explosions rocked the Egyptian resort city of Dahab at the height of the tourist season Monday night, April 24, killing at least 18 people and wounding more than 150 at just one hotel, according to the doctor who runs the Sinai peninsula rescue squad. Dr. Said Essa said he was headed to the scene of the blasts and that his casualty figures were for victims at the el-Khaleeg Hotel only. He said there were casualties from the other explosions but he had no details. Al-Jazeera television said one of the blasts hit a restaurant, and authorities said more than 20 ambulances and police cars were rushing to the el-Masbat section of the city. Terrorist attacks have killed nearly 100 people at several tourist resorts of Egypt's Sinai region in the past two years. Bombings in the resorts of Taba and Ras Shitan, near the Israeli border, killed 34 people in October 2004. Last July, suicide attackers in the resort of Sharm el-Sheik killed at least 64 people, mainly tourists. This is high tourist season in the region, and hotels all along the Egyptian coasts could be expected to be at near capacity, mainly with Europeans, Israelis, and expatriates living in Egypt.

Source: http://www.usatoday.com/news/world/2006-04-24-egypt-blasts_x.htm?POE=NEWISVA

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.